

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
 United States Patent and Trademark
 Office
 Box PCT
 Washington, D.C. 20231
 ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 17 April 2000 (17.04.00)	
International application No. PCT/DE99/02443	Applicant's or agent's file reference GR 98P2356P
International filing date (day/month/year) 04 August 1999 (04.08.99)	Priority date (day/month/year) 18 August 1998 (18.08.98)
Applicant HOFFMANN, Gerhard et al	

1. The designated Office is hereby notified of its election made:



in the demand filed with the International Preliminary Examining Authority on:

16 March 2000 (16.03.00)



in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
 34, chemin des Colombettes
 1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Kiwa Mpay

Telephone No.: (41-22) 338.83.38

**VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS**

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts GR 98P2356P	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; vertical-align: top;"> WEITERES VORGEHEN </td> <td style="width: 50%; vertical-align: top;"> siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5 </td> </tr> </table>		WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5			
Internationales Aktenzeichen PCT/DE 99/ 02443	Internationales Anmeldedatum (Tag/Monat/Jahr) 04/08/1999	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 18/08/1998		
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.				

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.



Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.



Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das



in der internationalen Anmeldung in Schriftlicher Form enthalten ist.



zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.



bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.



bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.



Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.



Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2.



Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3.



Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der Bezeichnung der Erfindung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der Zusammenfassung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1



wie vom Anmelder vorgeschlagen



weil der Anmelder selbst keine Abbildung vorgeschlagen hat.



weil diese Abbildung die Erfindung besser kennzeichnet.



keine der Abb.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 H04L9/30 H04L9/08 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 534 420 A (IBM) 31. März 1993 (1993-03-31) Spalte 5, Zeile 51 - Spalte 6, Zeile 20 Spalte 8, Zeile 56 - Spalte 10, Zeile 51 Spalte 3, Zeile 38 - Zeile 50 ---	1-20
P,X	WO 99 33219 A (KONINKL PHILIPS ELECTRONICS NV ; PHILIPS AB (SE)) 1. Juli 1999 (1999-07-01) Seite 5, Zeile 32 - Seite 9, Zeile 22 ---	1,11
A	CHRISTOPH RULAND: "Informationssicherheit in Datennetzen" 1993, DATACOM-VERLAG, BERGHEIM (DEUTSCHLAND) XP000863430 in der Anmeldung erwähnt Seite 79 - Seite 85 --- -/-	6,16



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

7. Januar 2000

Absendedatum des internationalen Recherchenberichts

17/01/2000

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Zucka, G

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	CHRISTOPH RULAND: "Informationssicherheit in Datennetzen" 1993 , DATACOM-VERLAG , BERGHEIM (DEUTSCHLAND) XP000863429 in der Anmeldung erwähnt Seite 68 -Seite 73 -----	2,7,12, 17

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 99/02443

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0534420	A	31-03-1993	US 5201000 A	06-04-1993
			CA 2075254 A	28-03-1993
			JP 2690004 B	10-12-1997
			JP 5224604 A	03-09-1993

WO 9933219	A	01-07-1999	AU 1348799 A	12-07-1999
			EP 0965200 A	22-12-1999

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

REC'D 12 DEC 2000

WIPO

PCT

4^T

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts GR 98P2356P	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE99/02443	Internationales Anmeldedatum (Tag/Monat/Jahr) 04/08/1999	Prioritätsdatum (Tag/Monat/Tag) 18/08/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/30		
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.		



- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 4 Blätter einschließlich dieses Deckblatts.

☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

 Diese Anlagen umfassen insgesamt Blätter.

- Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 16/03/2000	Datum der Fertigstellung dieses Berichts 07.12.2000
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Bevollmächtigter Bediensteter Zucka, G Tel. Nr. +31 70 340 4026 

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-13 ursprüngliche Fassung

Patentansprüche, Nr.:

1-20 ursprüngliche Fassung

Zeichnungen, Blätter:

1/3-3/3 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen Behörde in der Sprache: , zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, dass das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, dass die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE99/02443

- ☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-20
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-20
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-20
	Nein: Ansprüche	

2. Unterlagen und Erklärungen siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

Zu Punkt V

1. Es wird auf das folgende Dokument verwiesen:

D1 = EP-A-0 534 420 (IBM) 31. März 1993 (1993-03-31)

2. D1 offenbart (siehe Spalte 8, Zeile 56 - Spalte 10, Zeile 51) ein Verfahren zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar, welches einen geheimen Schlüssel sowie einen korrespondierenden öffentlichen Schlüssel umfaßt.
3. Der Gegenstand der unabhängigen Ansprüche 1 und 11 unterscheidet sich im wesentlichen dadurch von dem in D1 offenbarten Verfahren, daß der zweite öffentliche Schlüssel mit dem ersten öffentlichen Schlüssel identisch ist. Dies führt zu einer Vereinfachung.
4. Eine solche Vorgehensweise wird von den im Recherchenbericht aufgeführten Dokumenten weder offenbart noch nahegelegt. Eine erfinderische Tätigkeit wird somit anerkannt.
5. Der Gegenstand der abhängigen Ansprüche 2-10 und 12-20 ist demzufolge auch erfinderisch.

Zu Punkt VII

1. Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT werden in der Beschreibung weder der im Dokument D1 offenbarte einschlägige Stand der Technik noch dieses Dokument angegeben.
2. Die unabhängigen Ansprüche sind nicht in der zweiteiligen Form nach Regel 6.3 b) PCT abgefaßt. Im vorliegenden Fall erscheint die Zweiteilung jedoch zweckmäßig.

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GR 98P2356P	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE99/02443	International filing date (day/month/year) 04 August 1999 (04.08.99)	Priority date (day/month/year) 18 August 1998 (18.08.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/30		
Applicant SIEMENS AKTIENGESELLSCHAFT		

RECEIVED
MAY 3 - 2001
Technology Center 2100

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 4 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 16 March 2000 (16.03.00)	Date of completion of this report 07 December 2000 (07.12.2000)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE99/02443

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

- ☐ the international application as originally filed.
- ☒ the description, pages 1-13, as originally filed,
 pages _____, filed with the demand,
 pages _____, filed with the letter of _____,
 pages _____, filed with the letter of _____.
- ☒ the claims, Nos. 1-20, as originally filed,
 Nos. _____, as amended under Article 19,
 Nos. _____, filed with the demand,
 Nos. _____, filed with the letter of _____,
 Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig 1/3-3/3, as originally filed,
 sheets/fig _____, filed with the demand,
 sheets/fig _____, filed with the letter of _____,
 sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE 99/02443

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1 - 20	YES
	Claims		NO
Inventive step (IS)	Claims	1 - 20	YES
	Claims		NO
Industrial applicability (IA)	Claims	1 - 20	YES
	Claims		NO

2. Citations and explanations

1. This report makes reference to the following document:

D1 = EP-A-0 534 420 (IBM) 31 March 1993 (1993-03-31)

2. D1 discloses (see column 8, line 56 - column 10, line 51) a method for creating a secret communication key for a predetermined asymmetrical cryptographic key-pair, which comprises a secret key and a corresponding public key.
3. The subjects of independent Claims 1 and 11 differ essentially from the method disclosed in D1 in that the second public key is identical to the first public key. This results in simplification.
4. A procedure of this kind is neither known from, nor suggested by, the documents cited in the search report. An inventive step is therefore acknowledged.
5. The subjects of dependent Claims 2 - 10 and 12 - 20 are therefore inventive too.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE 99/02443

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to PCT Rule 5.1(a)(ii), the description does not cite document D1 or indicate the relevant prior art disclosed therein.
2. The independent claims are not drafted in the two-part form according to PCT Rule 6.3(b). In the present case, however, the two-part formulation seems appropriate.

Beschreibung

Verfahren und Anordnung zur Bildung eines geheimen Kommunika-
5 tionsschlüssels zu einem zuvor ermittelten asymmetrischen
kryptographischen Schlüsselpaar

Die Erfindung betrifft ein Verfahren und eine Anordnung zur
Bildung eines geheimen Kommunikationsschlüssels zu einem zu-
10 vor ermittelten asymmetrischen Schlüsselpaar.

Die Bildung eines asymmetrischen kryptographischen Schlüssel-
paars ist aus [1] bekannt.

15 Bei diesem Verfahren wird das RSA-Verfahren zur Bildung eines
kryptographischen Schlüsselpaars, welches einen geheimen
Schlüssel sowie einen korrespondierenden öffentlichen Schlüs-
sel umfaßt, gebildet.

20 Der geheime Schlüssel ist nur dem Benutzer bekannt, der öf-
fentliche Schlüssel kann allen Teilnehmern eines Kommunikati-
onsnetzes bekannt gemacht werden.

Bei der Erstellung einer digitalen Signatur zum Schutz der
25 Authentizität und Integrität elektronischer Daten unter-
schreibt der Benutzer die Daten mit seinem geheimen Schlüs-
sel. Die Verifikation der unterschriebenen digitalen Signatur
erfolgt unter Verwendung des zu dem geheimen Schlüssels kor-
respondierenden öffentlichen Schlüssel, wodurch die Authentizität
30 bzw. Integrität der digitalen Signatur von allen Kommunikati-
onspartnern überprüft werden kann, die Zugriff auf den
öffentlichen Schlüssel haben.

Die oben beschriebene sogenannte Public-Key-Technologie fin-
35 det insbesondere in der digitalen Kommunikation innerhalb ei-
nes Rechnernetzes (eine vorgebbare Anzahl von Rechnereinhei-

ten, die über ein Kommunikationsnetz miteinander verbunden sind) Anwendung.

Bei dem aus [1] bekannten Verfahren ist der Schutz des geheimen Schlüssels vor unberechtigter Kenntnisnahme eines Dritten für die Sicherheit der digitalen Signatur von essentieller Bedeutung.

Aus [2] ist es bekannt, den geheimen Schlüssel auf einem externen Medium zur Speicherung von Daten, beispielsweise einer Chipkarte, einer Diskette, etc. oder auf einer Festplatte zu speichern, wobei Schlüsseldaten unter Verwendung eines persönlichen Identifizierungscodes (Personal Identification Number, PIN) oder eines Paßworts, mit dem jeweils die Schlüsseldaten verschlüsselt werden, geschützt werden. Bei Nutzung dieser externen Medien sind jedoch Zugriffe auf die lokalen Ressourcen eines Benutzers notwendig. Dies ist jedoch gerade bei einer netzorientierten Infrastruktur von Netzcomputern oder Java-Applikationen nicht gewünscht.

Unter einem Netzcomputer ist ein Rechner zu verstehen, der mit weiteren Rechnern vernetzt ist.

Unter einer Java-Applikation ist ein Programm zu verstehen, welches in der Programmiersprache Java geschriebene Programme enthält.

Somit weist das aus [2] beschriebene Verfahren den Nachteil auf, daß der geheime Schlüssel auf einem externen Medium gespeichert werden muß und somit der geheime Schlüssel vor Mißbrauch nur schwer schützbar ist.

Eine Übersicht über Hash-Funktionen ist in [3] zu finden. Unter einer Hash-Funktion ist eine Funktion zu verstehen, bei der es nicht möglich ist, zu einem gegebenen Funktionswert einen passenden Eingangswert zu berechnen. Ferner wird einer beliebig langen Eingangszeichenfolge eine Ausgangszeichenfol-

ge fester Länge zugeordnet. Des weiteren können für die Hash-Funktion zusätzliche Eigenschaften gefordert werden. Eine solche zusätzliche Eigenschaft ist Kollisionsfreiheit, d.h. es darf nicht möglich sein, zwei verschiedene Eingangszeichenfolgen zu finden, die dieselbe Ausgangszeichenfolge ergeben.

Beispiele einer Hash-Funktion sind das Verfahren gemäß dem MD-2-Standard, das Verfahren gemäß dem MD-5-Standard, der Data Encryption Standard (DES), welcher ohne Verwendung eines Schlüssels durchgeführt wird, oder auch jede andere beliebige Hash-Funktion.

Ein als Verfahren nach Miller-Rabin bezeichnetes Verfahren, mit dem für eine Zahl überprüft werden kann, ob diese eine Primzahl darstellt, ist aus [4] bekannt.

Somit liegt der Erfindung das Problem zugrunde, einen geheimen Kommunikationsschlüssel zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar zu bilden, bei dem der geheime Schlüssel des asymmetrischen Schlüsselpaars nicht dauerhaft gespeichert werden muß.

Das Problem wird durch das Verfahren sowie durch die Anordnung mit den Merkmalen der unabhängigen Patentansprüche gelöst.

Bei dem Verfahren zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar, welches einen geheimen Schlüssel sowie einen korrespondierenden öffentlichen Schlüssel umfaßt, wurde bei der Ermittlung des Schlüsselpaars ein vorgebbare Startwert verwendet. Der Startwert wird einem Benutzer zur Verfügung gestellt. Der Benutzer gibt den Startwert in den Rechner ein und unter Verwendung des Startwerts wird der geheime Kommunikationsschlüssel gebildet. Der geheime Kommuni-

kationsschlüssel und der öffentliche Schlüssel bilden ein Kommunikationsschlüsselpaar.

- Die Anordnung zur Bildung eines geheimen Kommunikations-
- 5 schlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar, welches einen geheimen Schlüssel sowie einen korrespondierenden öffentlichen Schlüssel umfaßt, weist einen Prozessor auf, der derart eingerichtet ist, daß folgende Schritte durchführbar sind:
- 10 - bei der Ermittlung des Schlüsselpaars wurde ein vorgegebbarer Startwert verwendet,
- der Startwert wird einem Benutzer zur Verfügung gestellt,
- der Startwert wird von dem Benutzer in den Rechner eingegeben,
- 15 - unter Verwendung des Startwerts wird der geheime Kommunikationsschlüssel gebildet, wobei der geheime Kommunikationsschlüssel und der öffentliche Schlüssel ein Kommunikationsschlüsselpaar bilden.
- Ferner ist ein Eingabemittel vorgesehen zur Eingabe des
- 20 Startwerts durch den Benutzer.

Durch die Erfindung wird es möglich, den geheimen Schlüssel löschen zu können, ohne auf die starke Kryptographie der Public-Key-Technologie verzichten zu müssen.

- 25 Anschaulich kann der Startwert als ein von dem Benutzer vorgegebener oder auch zentral vorgegebener persönlicher Identifikationscode (Personal Identification Number PIN) oder als Paßwort angesehen werden, den der Benutzer in den Rechner
- 30 eingibt. Nach Eingabe des Paßworts bzw. der PIN wird unter Verwendung der des Paßworts bzw. der PIN als Startwert der geheime Kommunikationsschlüssel, d.h. der verglichen mit dem geheimen Schlüssel gleichlautende Schlüssel gebildet, der ein Schlüsselpaar, das Kommunikationsschlüsselpaar, gemeinsam mit
- 35 dem öffentlichen Schlüssel bildet.

Auf diese Weise wird mit der Erfindung eine Verschmelzung der für den Benutzer eines üblichen Rechnernetzes bzw. eines üblichen Rechners gewohnten Paßwort-Technologie mit der starken Kryptologie erreicht, ohne daß erhebliche Anstrengungen un-
5 ternommen werden müssen, um geheimes Schlüsselmaterial dauerhaft zu speichern.

Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

10

In einer Weiterbildung der Erfindung ist es vorgesehen, auf den Startwert eine Hash-Funktion anzuwenden, womit ein Wert gebildet wird, der schließlich zur Schlüsselgenerierung verwendet wird.

15

Weiterhin können zusätzliche Daten bei der Schlüsselgenerierung verwendet werden, die bevorzugt den Benutzer selbst charakterisieren.

20 Bevorzugt wird zur Bildung des kryptographischen Schlüssels das RSA-Verfahren zur Schlüsselgenerierung verwendet.

Als Hash-Funktion kann das Verfahren gemäß dem MD-5-Standard, dem MD-2-Standard oder auch dem Data Encryption Standard
25 (DES), eingesetzt als Einweg-Funktion eingesetzt werden.

Das Kommunikationsschlüsselpaar kann sowohl zur Verschlüsselung oder zur Integritätssicherung elektronischer Daten, zur Bildung einer digitalen Signatur über elektronische Daten
30 oder auch zur Authentifikation eines Benutzers eingesetzt werden, allgemein für eine beliebige kryptographische Operation, bei der die Public-Key-Technologie eingesetzt wird, wobei das gebildete Kommunikationsschlüsselpaar verwendet wird.

35 Zur Beschleunigung des Verfahrens ist es in einer Ausgestaltung vorteilhaft, bei der Bildung des geheimen Schlüssels einen Index zu speichern, der im weiteren als Beschleunigungs-

kennzahl bezeichnet wird. Mit der Beschleunigungskennzahl wird angegeben, wie oft Zahlen, ausgehend von dem Startwert, daraufhin überprüft worden sind, ob die jeweilige Zahl eine Primzahl darstellt oder nicht.

5

Zur Überprüfung der Eigenschaft, ob eine Zahl eine Primzahl darstellt, wird vorzugsweise das Verfahren nach Miller-Rabin eingesetzt.

- 10 Ein Ausführungsbeispiel der Erfindung ist in den Figuren dargestellt und wird im weiteren näher erläutert.

Es zeigen

- 15 Figur 1 ein Ablaufdiagramm, in dem die Verfahrensschritte des Ausführungsbeispiels dargestellt sind;

Figur 2 eine Skizze, in dem ein Rechnernetz mit einer Vielzahl miteinander gekoppelter Rechner dargestellt ist;

20

Figur 3 eine symbolische Skizze, in der die Vorgehensweise zur Ermittlung einer Primzahl ausgehend von einem Startwert dargestellt ist.

- 25 **Fig.2** zeigt eine Vielzahl von Rechnern 200, 210, 220, 230, 240, 250, die über ein Kommunikationsnetz 260 miteinander verbunden sind. Jeder Rechner 200, 210, 220, 230, 240, 250 weist jeweils mehrere Eingabemittel, d.h. eine Tastatur 206, 216, 226, 236, 246, 256, eine Maus 207, 217, 227, 237, 247, 30 257 oder einen Scanner (nicht dargestellt) oder auch eine Kamera (nicht dargestellt) auf. Über das jeweilige Eingabemittel wird über eine Eingangs-/Ausgangsschnittstelle 201, 211, 221, 231, 241, 251 einem Speicher 202, 212, 222, 232, 242, 252 die eingegebene Information zugeführt und gespeichert.
- 35 Der 202, 212, 222, 232, 242, 252 Speicher ist mit der Eingangs-/Ausgangsschnittstelle 201, 211, 221, 231, 241, 251 über einen Bus 204, 214, 224, 234, 244, 254 verbunden. Ebenso

mit dem Bus 204, 214, 224, 234, 244, 254 verbunden ist ein Prozessor 203, 213, 223, 233, 243, 253, der derart eingerichtet ist, daß die im weiteren beschriebenen Verfahrensschritte durchführbar sind.

5

Die Rechner 200, 210, 220, 230, 240, 250 kommunizieren über das Kommunikationsnetz 260 gemäß dem Transport Control Protocol/Internet Protocol (TCP/IP).

- 10 Ferner ist in dem Kommunikationsnetz 260 eine Zertifizierungseinheit 270 vorgesehen, mit der für jeweils einen öffentlichen Schlüssel ein Zertifikat ausgestellt wird, so daß der öffentliche Schlüssel vertrauenswürdig ist für eine Kommunikation auf der Basis der Public-Key-Technologie.

15

Ein Benutzer 280 gibt in einen ersten Rechner 200 ein beliebiges vorgebbares Wort (PIN, Paßwort), welches nur dem Benutzer bekannt ist, ein (Schritt 101, vgl. Fig.1).

- 20 Von dem ersten Rechner 200 wird gemäß dem RSA-Verfahren ein asymmetrisches kryptographisches Schlüsselpaar generiert, wie im folgenden beschrieben.

- 25 Der von dem Benutzer 280 eingegebene Wert 102 sowie Zusatzdaten 103, die den Benutzer 280 charakterisieren, zum Beispiel Benutzername, Personalnummer, Terminal-Adresse, etc. werden einer Hash-Funktion zugeführt (Schritt 104).

- 30 Eine Übersicht über Hash-Funktionen ist in [3] zu finden. Unter einer Hash-Funktion ist eine Funktion zu verstehen, bei der es nicht möglich ist, zu einem gegebenen Funktionswert einen passenden Eingangswert zu berechnen. Ferner wird einer beliebig langen Eingangszeichenfolge eine Ausgangszeichenfolge fester Länge zugeordnet. Des weiteren können für die Hash-
- 35 Funktion zusätzliche Eigenschaften gefordert werden. Eine solche zusätzliche Eigenschaft ist Kollisionsfreiheit, d.h. es darf nicht möglich sein, zwei verschiedene Eingangszei-

chenfolgen zu finden, die dieselbe Ausgangszeichenfolge ergeben.

5 Beispiele einer Hash-Funktion sind das Verfahren gemäß dem MD-2-Standard, das Verfahren gemäß dem MD-5-Standard, der Data Encryption Standard (DES), welcher ohne Verwendung eines Schlüssels durchgeführt wird, oder auch jede andere beliebige Hash-Funktion.

10 Der durch die Hash-Funktion gebildete Wert wird als Basiswert BW zur Bildung zweier Primzahlen verwendet, wie in Fig.3 symbolisch dargestellt ist.

15 Wie in Fig.3 dargestellt, wird ausgehend von dem Basiswert BW jeweils für einen Wert W_i ($i = 1, \dots, n$) in einem iterativen Verfahren überprüft, ob der jeweilige Wert eine Primzahl darstellt oder nicht (Schritt 301).

20 Als Verfahren zur Überprüfung der Eigenschaft Prim für eine Zahl wird das Verfahren gemäß Miller-Rabin eingesetzt, welches in [4] beschrieben ist.

25 Wird für eine Zahl festgestellt, daß die Zahl keine Primzahl ist, so wird die Zahl um einen vorgebbaren Wert, vorzugsweise um den Wert 2 erhöht (Schritt 302) und der Test auf die Eigenschaft „Prim“ wird wiederholt (Schritt 301). Dieses Vorgehen wird solange wiederholt, bis zwei Primzahlen, eine erste Primzahl p und eine zweite Primzahl q ermittelt worden sind.

30 Als Index wird eine Zahl bezeichnet, mit der angegeben wird, wie oft ausgehend von dem Basiswert PW die Zahl um den vorgegebenen Wert erhöht werden muß, bis man zu der ersten Primzahl p bzw. zu der zweiten Primzahl q gelangt.

35 Ergebnis des in Fig.3 dargestellten Verfahrens sind zwei Primzahlen p und q , die zur Schlüsselgenerierung gemäß dem RSA-Verfahren (Schritt 105) eingesetzt werden.

Die Primzahlen p und q weisen üblicherweise eine Länge mehrerer 100 Bit auf.

- 5 Aus den Primzahlen p und q wird ein Modulus n gemäß folgender Vorschrift gebildet:

$$n = p * q. \quad (1)$$

- 10 Ferner wird eine Zwischengröße $\phi(n)$ gemäß folgender Vorschrift gebildet:

$$\phi(n) = (p-1) * (q-1). \quad (2)$$

- 15 Ein geheimer Schlüssel d wird nun derart gewählt, daß der geheime Schlüssel d teilerfremd zu $\phi(n)$ ist. Ein öffentlicher Schlüssel e wird derart bestimmt, daß folgende Vorschrift erfüllt ist:

$$20 \quad e * d \bmod \phi(n) = 1. \quad (3)$$

Der Wert d ist der geheime Schlüssel und darf keinem Dritten bekannt gemacht werden.

- 25 Somit ist durch die Schlüsselgenerierung (Schritt 105) ein privater Schlüssel d (Schritt 106) und ein öffentlicher Schlüssel e (Schritt 107) gebildet worden.

- 30 Die beiden Schlüssel d , e bilden ein zueinander korrespondierendes kryptographisches Schlüsselpaar, welches für eine beliebige kryptographische Operation, d.h. zur Verschlüsselung, zur Entschlüsselung oder auch zur digitalen Signatur oder zur Authentifikation eingesetzt wird (Schritt 108).

- 35 Nach Bildung des Schlüsselpaares d , e gemäß dem oben beschriebenen Verfahren wird der geheime Schlüssel d gelöscht.

Der öffentliche Schlüssel e wird der Zertifizierungsinstanz 280 zugeführt. Von der Zertifizierungsinstanz 280 wird ein Zertifikat $Certe$ über den öffentlichen Schlüssel e gebildet und das Zertifikat $Certe$ des öffentlichen Schlüssels e wird
5 in einem öffentlich zugänglichen Verzeichnis 290 gespeichert.

Somit kann jeder Kommunikationsteilnehmer in dem Kommunikationsnetz 280 auf den öffentlichen Schlüssel e über das Zertifikat $Certe$ des öffentlichen Schlüssels e zugreifen.
10
Der geheime, zu dem öffentlichen Schlüssel e korrespondierende Schlüssel d ist in dem ersten Rechner 200 gelöscht.

Jedesmal, wenn der Benutzer 280 auf der Basis des Schlüssel-
15 paares eine Kommunikation beginnen will, bzw. eine kryptographische Operation unter Verwendung eines solchen Schlüssel-
paares durchführen will, gibt der Benutzer 208 in den ersten Rechner 200 seinen Startwert (PIN, Paßwort) ein und der
Startwert 102 wird wie oben beschrieben wiederum mit Zusatz-
20 daten 103 versehen, einer Hash-Funktion unterzogen
(Schritt 104) und es werden entweder ausgehend von dem Basiswert BW zwei Primzahlen p und q ermittelt oder es wird ein
gespeicherter Index, wie oben beschrieben, ausgelesen oder
ebenfalls von dem Benutzer 280 eingegeben und daraus wird ein
25 geheimer Kommunikationsschlüssel gebildet, der dem geheimen,
zuvor gebildeten jedoch wieder gelöschten Schlüssel d entspricht.

Auf diese Weise ist ein Kommunikationsschlüsselpaar gebildet
30 worden, welches den geheimen Kommunikationsschlüssel sowie
den korrespondierenden öffentlichen Schlüssel e umfaßt. Damit
kann jeweils für eine Kommunikationssitzung von einem Benutzer
aktuell der geheime Kommunikationsschlüssel erzeugt werden,
womit es möglich ist, starke Public-Key-Technologie einzusetzen,
35 ohne den geheimen Schlüssel auf einer Chipkarte
speichern zu müssen.

Das somit gebildete Kommunikationsschlüsselpaar d, e wird verwendet zur Verschlüsselung von Klartext 109 mit dem öffentlichen Schlüssel e und der Entschlüsselung der elektronischen, verschlüsselten Daten 110 mit dem geheimen Kommunikationsschlüssel.

Die Verarbeitung von Klartext 109, d.h. für jedermann lesbare elektronische Daten 109 sowie verschlüsselte elektronische Daten 110 sind in Fig.1 symbolisch dargestellt, wobei die Kommunikationsrichtung jeweils durch einen Pfeil hin bzw. von dem Block, welcher eine kryptographische Operation 108 darstellt, beschreibt.

Die Verschlüsselung bzw. Entschlüsselung erfolgt gemäß folgenden Vorschriften:

$$m^e \bmod n = c, \quad (4)$$

wobei mit

20

- m eine Menge von 512 Bit elektronischer Daten 109, die es zu verschlüsseln gilt,
- c verschlüsselte elektronische Daten 110,

25 bezeichnet werden.

Die Entschlüsselung der verschlüsselten elektronischen Daten c erfolgt gemäß folgender Vorschrift:

$$m = c^d \bmod n. \quad (5)$$

Im weiteren werden einige Alternativen des oben dargestellten Ausführungsbeispiels erläutert:

35 Das Verfahren kann sowohl zur Verschlüsselung als auch zur Integritätssicherung oder auch zur digitalen Unterschrift elektronischer Daten eingesetzt werden.

Ferner kann die Erfindung im Bereich sicherer elektronischer Mail-Systeme eingesetzt werden.

- 5 Der Startwert 102 muß bei der Generierung des Schlüsselpaars zu Beginn des Verfahrens nicht unbedingt von dem Benutzer eingegeben werden, sondern er kann auch von einer zentralen Einheit, welche das Schlüsselpaar generiert, dem Benutzer vorgegeben werden.
- 10 Somit hat sich der Benutzer lediglich ein Paßwort bzw. eine PIN zu merken und es ist nicht mehr erforderlich, einen geheimen kryptographischen Schlüssel sicher zu speichern, beispielsweise auf einer Chipkarte, was mit entsprechenden Risiken und mit erheblichem Aufwand verbunden ist.
- 15

Anstelle einer Hash-Funktion kann im Rahmen der Erfindung jede beliebige Einwegfunktion eingesetzt werden.

Im Rahmen dieses Dokuments wurden folgende Veröffentlichungen zitiert.

- 5 [1] C. Ruland, Informationssicherheit in Datennetzen,
ISBN 3-89238-081-3, DATACOM-Verlag, S. 79 - 85, 1993
- [2] D. Longley und M. Shain, Data & Computer Security,
Dictionary of standards concepts and terms, Stockton
Press, ISBN 0-333-42935-4, S. 317, 1987
- 10 [3] C. Ruland, Informationssicherheit in Datennetzen,
ISBN 3-89238-081-3, DATACOM-Verlag, S. 68 - 73, 1993
- 15 [4] A. J. Menezes, P. van Oorschot and S. Vanstone, Handbook
of Applied Cryptography, CRC Press, ISBN 0-8493-8523-7,
S. 138 - 140, 1997

Patentansprüche

1. Verfahren zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar, welches einen geheimen Schlüssel sowie einen korrespondierenden öffentlichen Schlüssel umfaßt, durch einen Rechner,
- 5 a) bei dem bei der Ermittlung des Schlüsselpaars ein vorgebarer Startwert verwendet wurde,
- 10 b) bei dem der Startwert einem Benutzer zur Verfügung gestellt wird,
- c) bei dem der Benutzer den Startwert in den Rechner eingibt,
- d) bei dem unter Verwendung des Startwerts der geheime Kommunikationsschlüssel gebildet wird, wobei der geheime Kommunikationsschlüssel und der öffentliche Schlüssel ein asymmetrisches kryptographisches Kommunikationsschlüsselpaar bilden.
- 15
2. Verfahren nach Anspruch 1,
- 20 bei dem der Startwert einer Hash-Funktion zugeführt wird und der durch die Hash-Funktion gebildete Wert bei der Ermittlung des Schlüsselpaars sowie des Kommunikationsschlüsselpaars verwendet wird.
- 25
3. Verfahren nach Anspruch 1 oder 2,
- bei dem bei der Bildung des Schlüsselpaars und des Kommunikationsschlüsselpaars Zusatzdaten, die den Benutzer charakterisieren, verwendet werden.
- 30
4. Verfahren nach einem der Ansprüche 1 bis 3,
- bei dem ausgehend von dem Startwert eine Primzahl ermittelt wird, wobei jeweils in einem iterativen Verfahren solange daraufhin geprüft wird, ob die jeweils überprüfte Zahl eine Primzahl ist und wenn dies der Fall ist, ein Index gespeichert wird, mit dem eine Anzahl von Zahlen bezeichnet wird,
- 35

die auf ihre Eigenschaft hin, ob sie eine Primzahl sind, überprüft worden sind, gespeichert wird,

- sonst eine weitere Zahl ausgehend von der überprüften Zahl ausgewählt wird und der Index um eine vorgegebene Zahl erhöht wird,

- bei dem nach der Bildung des Kommunikationsschlüsselpaars die verwendete Primzahl gelöscht wird,

- bei dem bei der neuen Bildung eines Kommunikationsschlüsselpaars jeweils der Index und der Startwert verwendet werden zur Bildung des geheimen Kommunikationsschlüssels.

5. Verfahren nach Anspruch 4,

bei dem der Test, ob eine Zahl eine Primzahl ist, gemäß dem Verfahren nach Miller-Rabin erfolgt.

6. Verfahren nach einem der Ansprüche 1 bis 5,

bei dem die Schlüssel gemäß dem RSA-Verfahren gebildet werden.

7. Verfahren nach einem der Ansprüche 2 bis 6,

bei dem die Hash-Funktion eines der folgenden Verfahren ist:

- MD-5-Verfahren,

- MD-2-Verfahren,

- das Verfahren gemäß dem Data Encryption Standard (DES) als Einweg-Funktion.

8. Verfahren nach einem der Ansprüche 1 bis 7,

eingesetzt zur Verschlüsselung elektronischer Daten mit dem geheimen Kommunikationsschlüssel.

9. Verfahren nach einem der Ansprüche 1 bis 7,

eingesetzt zur Bildung einer digitalen Signatur über elektronische Daten unter Verwendung des geheimen Kommunikationsschlüssels.

10. Verfahren nach einem der Ansprüche 1 bis 7,

eingesetzt zur Authentifikation unter Verwendung des geheimen Kommunikationsschlüssels.

11. Anordnung zur Bildung eines geheimen Kommunikations-
5 schlüssels zu einem zuvor ermittelten asymmetrischen krypto-
graphischen Schlüsselpaar, welches einen geheimen Schlüssel
sowie einen korrespondierenden öffentlichen Schlüssel umfaßt,
mit einem Prozessor, der derart eingerichtet ist, daß folgen-
de Schritte durchführbar sind:
- 10 - das Schlüsselpaar wurde unter Verwendung eines vorgebbaren
Startwerts ermittelt,
- der Startwert wird einem Benutzer zur Verfügung ge-
stellt,
- der Startwert wird von dem Benutzer in den Rechner ein-
15 gegeben,
- unter Verwendung des Startwerts wird der geheime Kommu-
nikationsschlüssel gebildet, wobei der geheime Kommu-
nikationsschlüssel und der öffentliche Schlüssel ein Kom-
munikationsschlüsselpaar bilden, und
20 mit einem Eingabemittel zur Eingabe des Startwerts durch den
Benutzer.

12. Anordnung nach Anspruch 11,
bei der der Prozessor derart eingerichtet ist, daß der Start-
25 wert einer Hash-Funktion zugeführt wird und der durch die
Hash-Funktion gebildete Wert bei der Ermittlung des Schlüs-
selpaars sowie des Kommunikationsschlüsselpaars verwendet
wird.

- 30 13. Anordnung nach Anspruch 11 oder 12,
bei der der Prozessor derart eingerichtet ist, daß bei der
Bildung des Schlüsselpaars und des Kommunikationsschlüssel-
paars Zusatzdaten, die den Benutzer charakterisieren, verwen-
det werden.

- 35 14. Anordnung nach einem der Ansprüche 11 bis 13,
bei der der Prozessor derart eingerichtet ist, daß

- ausgehend von dem Startwert eine Primzahl ermittelt wird, wobei jeweils in einem iterativen Verfahren solange daraufhin geprüft wird, ob die jeweils überprüfte Zahl eine Primzahl ist und wenn dies der Fall ist, ein Index gespeichert wird, mit dem eine Anzahl von Zahlen bezeichnet wird, die auf ihre Eigenschaft hin, ob sie eine Primzahl sind, überprüft worden sind, gespeichert wird,
- sonst eine weitere Zahl ausgehend von der überprüften Zahl ausgewählt wird und der Index um eine vorgegebene Zahl erhöht wird,
- nach der Bildung des Kommunikationsschlüsselpaars die verwendete Primzahl gelöscht wird,
- bei der neuen Bildung eines Kommunikationsschlüsselpaars jeweils der Index und der Startwert verwendet werden zur Bildung des geheimen Kommunikationsschlüssels.

15. Anordnung nach Anspruch 14, bei der der Prozessor derart eingerichtet ist, daß der Test, ob eine Zahl eine Primzahl ist, gemäß dem Verfahren nach Miller-Rabin erfolgt.

16. Anordnung nach einem der Ansprüche 11 bis 15, bei der der Prozessor derart eingerichtet ist, daß die Schlüssel gemäß dem RSA-Verfahren gebildet werden.

17. Anordnung nach einem der Ansprüche 12 bis 16, bei der der Prozessor derart eingerichtet ist, daß die Hash-Funktion eines der folgenden Verfahren ist:

- MD-5-Verfahren,
- MD-2-Verfahren,
- das Verfahren gemäß dem Data Encryption Standard (DES) als Einweg-Funktion.

18. Anordnung nach einem der Ansprüche 11 bis 17, eingesetzt zur Verschlüsselung elektronischer Daten mit dem geheimen Kommunikationsschlüssel.

18

19. Anordnung nach einem der Ansprüche 11 bis 17, eingesetzt zur Bildung einer digitalen Signatur über elektronische Daten unter Verwendung des geheimen Kommunikationsschlüssels.

5

20. Anordnung nach einem der Ansprüche 11 bis 17, eingesetzt zur Authentifikation unter Verwendung des geheimen Kommunikationsschlüssels.

Zusammenfassung**Verfahren und Anordnung zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar**
5

Nachdem ein Schlüsselpaar mit einem öffentlichen Schlüssel und einem korrespondierenden geheimen Schlüssel ausgehend von einem Startwert ermittelt wurde, wird der Startwert einem Benutzer zur Verfügung gestellt. Der geheime Schlüssel kann gelöscht werden. Wenn der Benutzer eine auf der Public-Key-Technologie basierende kryptographische Operation durchführen möchte, gibt der Benutzer den Startwert in einen Rechner ein und unter Verwendung des Startwerts wird ein geheimer Kommunikationsschlüssel gebildet, der dem zuvor gebildeten, seitdem gelöschten geheimen Schlüssel entspricht.

10
15

Sign. Figur 1

FIG 1

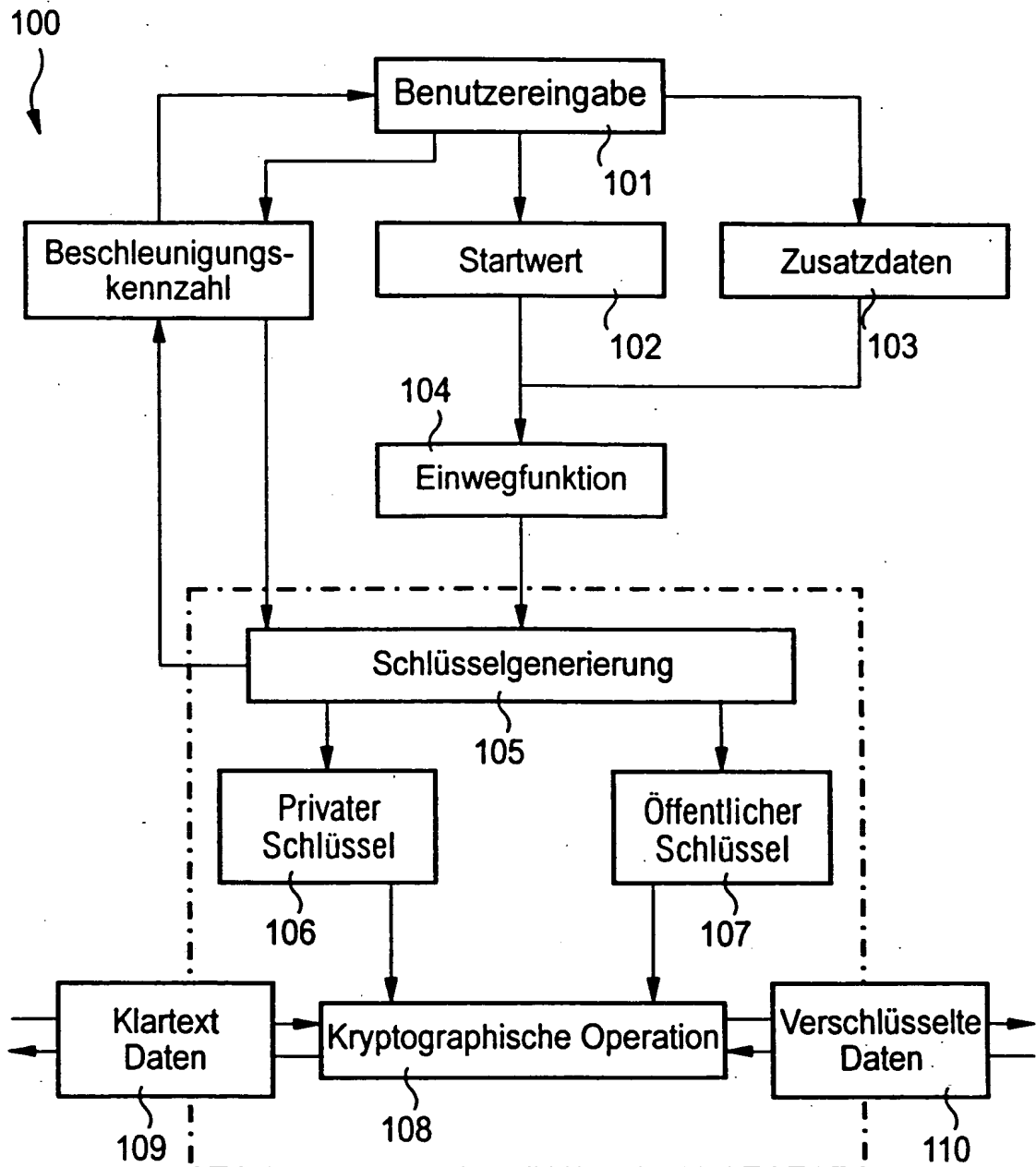


FIG 2

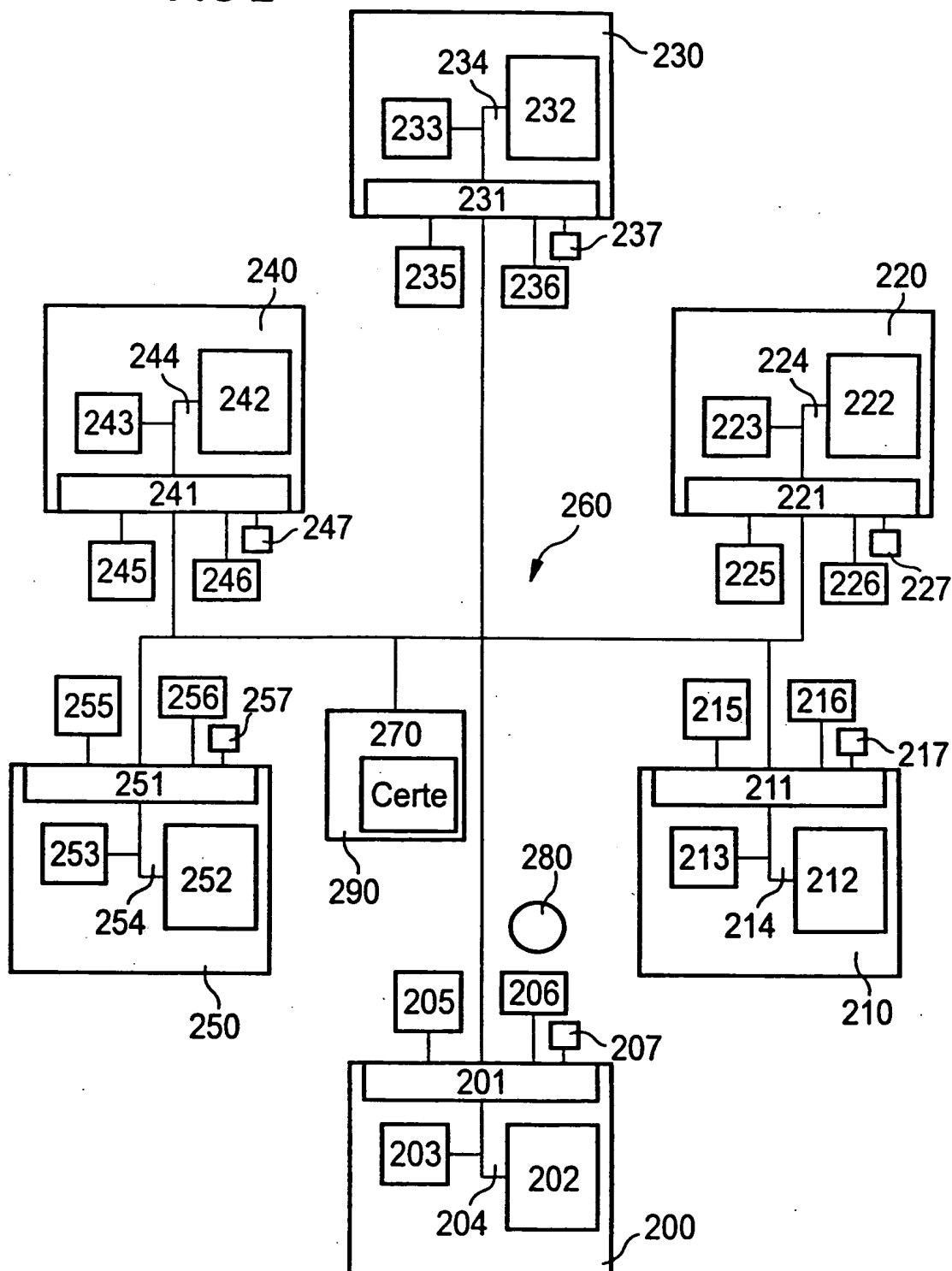


FIG 3

